Resilient System, or a Pyrrhic Victory?

Cyber Resilience Conference

Denver, Colorado

August 19-21, 2014

Michael A. VanPutte, Ph.D., CISSP

MOD-2 Systems
michael@mvanputte.com

Distribution Statement “A” (Approved for public release. Distribution unlimited.)The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Bounds

- **Goal: Explain cyber adversary "attacker" (someone exploiting our reliance on cyberspace), and their resiliency to defender's actions.**

- **Premise:**
  - **Developing robust resilient cyber solutions that leaders will deploy in operational environments requires us to think holistically**
    - **If you're trying to build systems resilient in the face of threats, you need to understand the threats**

- **Disclaimer.**
  - **I'm not talking about gathering intelligence on specific threats, individuals, groups.**

If you are going to build resilient systems or defenses then you need to understand and anticipate the full spectrum of adversaries, and attacker's technical, social, procedural capabilities, and goals.

Observations

1 - Avoid security buzzwords and myths

- Risk Management.
- Advanced Persistent Threats (APT)
- “Stupid User”
- Cyber War

2 - Attacking is a mindset, not a technology

3 – Our actions make attackers more resilient and encourage attackers

4 - Resilient system must evolve

5 - Resilient systems must protect all of your missions, not the network and systems

6 - Attacker will use transitivity against you

7 - Attackers will react to your actions

8 - Your most dangerous opponents may never touch your technology

Questions?

Michael A. VanPutte, Ph.D.
MOD-2 Systems
michael@mvanputte.com

References

- S. Frei, Correlation of Detection Failures, NSS Labs, 2013. Retrieved from https://www.nsslabs.com/news/press-releases/are-security-professionals-overconfident-%E2%80%9Cdefense-depth%E2%80%9D on 1 February 2014.
- Xue reports on 165 vulnerabilities over a four year period in anti-virus technologies, concluding "[It] is clear that antivirus software can be targeted just likes other components or services of computer systems." Feng Xue, Attacking Antivirus, retrieved from http://sebug.net/paper/Meeting-Documents/syscanhk/AttackingAV_BHEU08_WP.pdf on May 20, 2014.
- Heartbleed exploit uses a hole in Secure Socket Layer tools that were designed to allow secure information sharing on the Internet. http://www.cnn.com/2014/04/08/tech/web/heartbleed-openssl/
- Verizon Data Breach Investigation Report, 2013, p6. Available at http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf?r=72
- Plutarch. Parellel Lives: Pyrrhus, 23.6. Available at http://penelope.uchicago.edu/Thayer/E/Roman/Texts/Plutarch/Lives/Pyrrhus